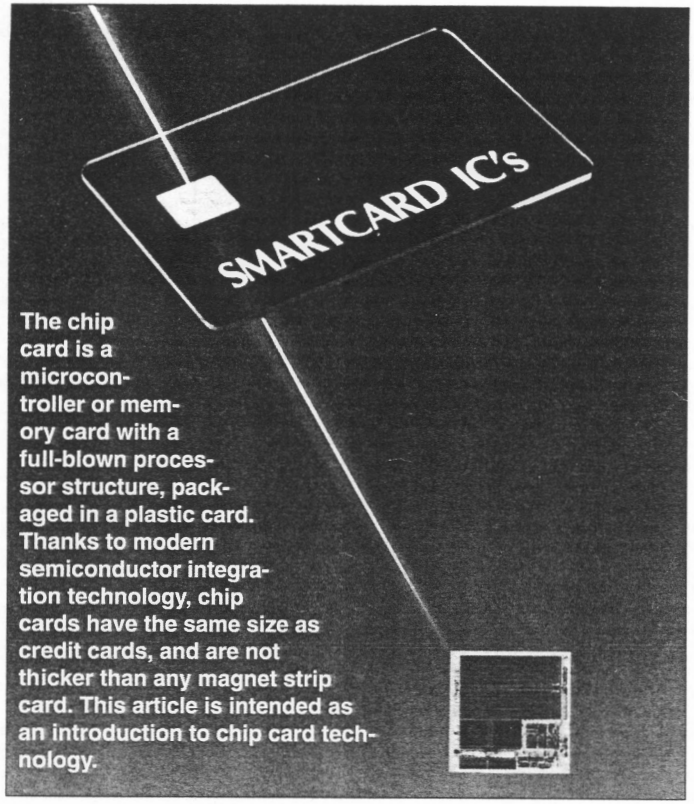
CHIP CARDS



The chip card is a microcontroller or memory card with a full-blown processor structure, packaged in a plastic card. Thanks to modern semiconductor integration technology, chip cards have the same size as credit cards, and are not thicker than any magnet strip card. This article is intended as an introduction to chip card technology.

Based on an article by J. Heine

CHIP cards with a variety of appearances and functions have been around since the middle of the nineteen seventies. Today, they are used increasingly in, for instance, telephone booths (though not yet in the UK) and personnel identification and work time logging systems in large plants and office buildings. In some cases, they are also used for electronic financial transactions. In the near future, further measures towards application-independent, international, standardization of the chip card is sure to give a tremendous boost to the number of applications. This will be helped by much reduced productions cost, which goes hand in hand with high production volumes. Also, a combined chipcard/magnet strip card will soon be unveiled.

The primary function of a chip card is to help identify the rightful owner, or, with non-personalized cards, to grant the user a certain service for which a remuneration is due that is within the limits of the 'value' of the card. In this respect, chip cards are the successors of the widespread 'flexible friend', the magnet strip card issued by banks and credit card organizations. The requirements as regards physical and electrical characteristics of the chip card are laid down in ISO standard 7816, part 3.

Construction of a chip card

The generic name 'chip card' is used to cover the following products:

- Smart Card
- Memory Card
- Processor Card
- Intelligent Card
- IC card

These different names already hint at differences as regards function and interion. According to the IS dard, the name 'IC Card' sho d to denote all members of the chip card family.

Magnet strip cards with their passiv function and small memory capacit (342 bytes) are easily read, copied and forged. By contrast, chip cards, by virtue of their much larger memory capacity (up to 32 KByte), built-in intelligence and access lock, offer a much higher degree of safety against unauthorized use. Yet, they are relatively cheap to produce.

Production

The chip card has the same size as a bank or credit card: 85.6×54×0.76 mm. For mobile telephones and other applications where space is restricted, so-called 'Plug-in SIM®' cards are available with a size of 18×28×0.76 mm. The chip proper has a size of 10×10 mm^2, and is embedded in plastic carrier material. Because of the flexibility of the card and other external factors, the carrier 'floats' inside a clearance in the plastic carrier. The chip carrier element is produced by covering both sides of a foil with copper foil. Next, the contacts and the layout are etched (**Fig. 1**), and subsequently through-contacted. Onto this composite foil, an equalizing foil is laminated, from which the clearances for the chip contacts are punched. The chip is secured on to the equalizing foil with the aid of silicon rubber cement, connected to the conducting foil, and subsequently covered by another foil. The rear side of the conducting foil contains the contacts (shown in the form of a punch-out pin feed strip in the background of Fig. 1), which later form the contacts to the outside world. A further layer of foil, which has clearances of the size of the contact elements, is secured at the contact element side of the conducting foil. The finished carrier element is punched out of a larger sheet, and inserted into the card, which consists of several layers of PVC foil. These make the card resistant against high temperatures, high humidity, and chemicals. However, direct heat transfer to the card, as well as electrical noise at the chip contacts (ESD) and excessive strain caused by bending, should be avoided.

Block diagram

The basic elements in a chip card are shown in **Fig. 2**. They include:

- a microcontroller (CPU)
- a scratch memory (RAM)
- a program memory (ROM)
- a data memory (EPROM or EEPROM)
- an input/output block (I/O)

Depending on the application, memory cards may be preferred over processor cards. In the long term, however, the trend will be towards combination cards

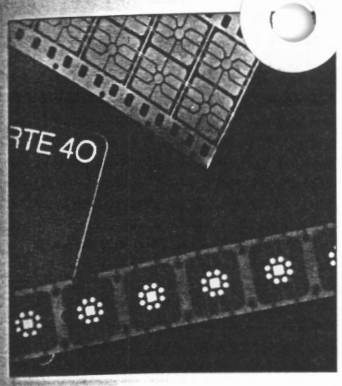


Fig. 1. Building blocks of a chip card: in front, the etched chip carrier element, in the centre, the (unfinished) card, and in the background, the punching tape.

and standardized readers which accept all types of card. Two of the world's major credit card organizations, VISA and Eurocard, already supply combination cards which allow users to make credit card purchases in the usual way using the magnetic strip system, as well as make telephone calls with automatic payment via their account. In response to this trend, telephone booths in many countries are rapidly upgraded to accept these cards.

Because of the standardized protocol as regards access, and because their 'intelligence' allows them to be tailored to future protocols, processor-type chip cards are generally considered the best candidates to pioneer a universally usable and global chip card technology.

Access

The card has six to eight gold-plated contacts with an effective contact area of

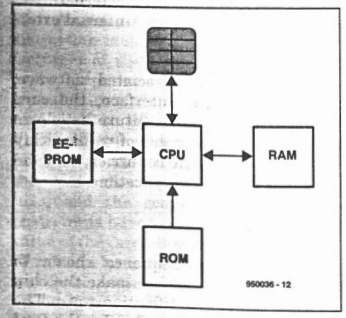


Fig. 2. The basic architecture of a chip card is fully equivalent to that of a microcontroller system.

1.7×2 mm^2. The two possible positions of the contacts on the card are accurately defined. The position used depends on that of the magnet strip and the printed area.

Chip card readers (also called card terminals) are currently available in a number of versions, from simple ones with spring-operated pin contacts, to zero-insertion force types with end switches. The ultimate, however, is the motor hybrid card reader which automatically moves cards into the contact position, and ejects them after reading. **Figure 7** shows a simple and therefore reasonably priced card reader unit with pin contacts and an end switch (which turns the reader on and off).

The position of the contact area of a telephone card with a fixed number of 'credit units' (i.e., cost pulses) is shown in **Fig. 3**. The telephone card is powered by a supply voltage of 5 V (**Table 1**) via contacts C1 and C5 (GND), and has an on-card voltage step-up converter for the EEPROM programming voltage. A clock signal (CLK) is applied to the card via contact C3 to enable serial data to be conveyed bidirectionally via contact C7 (I/O). Contact C6 is rarely used in modern card readers. It supplies an external programming voltage (V_{pp}), which is applied after the card has been identified. Only a few types of (by now obsolete) cards require this programming voltage.

Although the functions of contacts C4 and C8 are 'reserved' according to the standard, they are not used on most cards. Contact C2 functions as a reset input which allows the 'intelligent' contact with the card to be established, followed by an identification operation

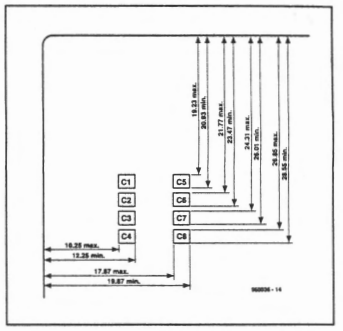


Fig. 3. Location of the eight-way contact are on the card.

contact	designation	contact	designation
C1	VCC (Supply Voltage)	C5	GND (Ground)
C2	RST (Reset)	C6	VPP (Programming Voltage)
C3	CLK (Clock Signal)	C7	I/O (Input/Output)
C4	Reserved	C8	Reserved

950036 - 18

Table 1. Functions of the electrical contacts on the chip card.

(both according to a protocol described further on).

Programming

Table 2 lists a number of the largest and best known manufacturers of chip cards. Philips and OKI concentrate on processor cores for which extensive development systems are available, and complete these cores with arithmetic processors capable of processing secu-

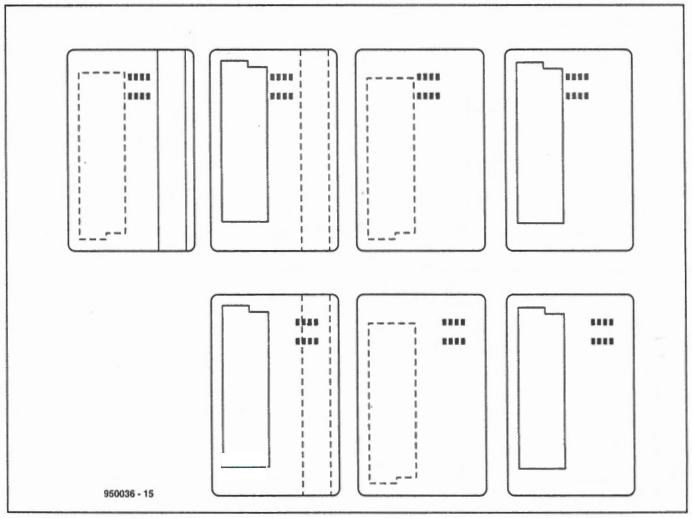


Fig. 4. Possible locations of electrical contacts and magnet strips on combination cards.

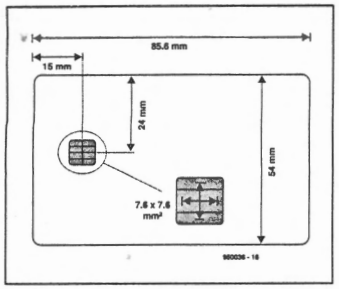


Fig. 5. Dimensions of a disposable phonecard with a fixed equivalent value.

Manufacturer Type	CPU		ROM	EEPROM
Siemens SLE 44xx	8 Bit 8051 derivative	128 Byte	4 kByte	2 kByte
Motorola 68HC05xx	8 Bit 6805	128 Byte	6 kByte	3 kByte
SGS ST9	8 Bit 6805 derivative	256 Byte	20 kByte	1.5 kByte
Toshiba TOSMART	8 Bit Z80 derivative	512 Byte	8 kByte	8 kByte
Hitachi H8/310	8 Bit H8	256 Byte	10 kByte	8 kByte
Philips 83C852	8 Bit 80C51 derivative	256 Byte	6 kByte	2 kByte
OKI MSM627xxx	8 Bit 8051 derivative	448 Byte	14 kByte	16 kByte

950036 - 19

Table 2. Overview of microcontroller products and their main features related to chip cards

rity-sensitive data using encryption algorithms like DES (data encryption standard).

Chip cards have astoundingly large memory areas. Today, there is nothing special about 32 Kbytes of EEPROM, 32 Kbytes of ROM and 512 bytes of RAM contained in a chip card. Such large memories speed up arithmetic operations considerably, and are a must considering that cards are used with 'signatures' having a length of 512 bits, and algorithms with an iteration depth of up to 32 bits to encrypt a single block of clear text (64 Bytes). The large ROM area provides sufficient space for program, look-up and encryption tables. The EEPROM locations are usually reserved for the option of running several applications on a single card.

To the electronics hobbyist, only the all-EEPROM based chip cards are of possible interest. These contain a processor running a program which only arranges the data transfer to and from the EEPROM, and takes care of the serial communication section. Using these basic utilities, certain (expired) intelligent phonecards may be given a 'second application' using the read-only mode. Most ordinary phonecards, however, are useless once their credit is used up.

Identification

The way chip cards identify themselves is standardized and referred to as 'answer-to-reset' in ISO 7816-3. The card reads a ROM-resident 128-bit wide recognition word (max. 256 bytes with other cards) containing, amongst others, manufacturer data (protocol T=1). This word is copied to the card reader via the I/O pin. The designation T=_ refers to a special protocol which is also specified in the ISO standard. Currently, there is T=0, T=1 and T=14.

Cards and countries

Unfortunately, the use of one and the same chip card for a single application (for instance, making use of a public telephone anywhere in Europe) is hindered by difficulties in equalizing (to a certain degree) the tariff structures used in the telecommunications field, as well as by the lack of identical concepts for secure storage of the card's residual value. The two problems are caused by the fact that a number of currently applied protocols are tailored to one application only. Market areas formed by country-specific users have caused the introduction of different protocols and sub-protocols into the standard.

Although the 'answer-to-reset' procedure is able to identify the protocol used by the card, that does not mean that the reader system actually supports that particular protocol. Consequently, it is not yet possible to speak of overall compatibility or, indeed, of the cross-frontier and totally application-independent chip card.

Compatibility so far only means that any chip card's contact area is to the ISO standard, and that the reader performs a standard identification check when the card is inserted.

Answer-to-reset obviously works on processor cards as well as on their simpler counterparts, memory cards. The identification word provides information on electrical and interface data including

- position of the MSB in the dataword;
- communication protocol;
- clock frequency (internal/external);
- programming voltage (internal/external).

By modifying the associated software, and, possibly, the interface, the card reader presented in a future article in this magazine is capable of reading chip cards from different countries, and designed for different applications.

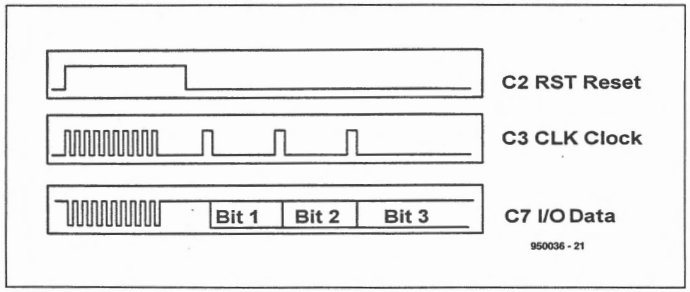


Fig. 6. Answer-to-reset pulse sequence.

Protocol

The initialization sequence shown in **Fig. 6** should be used to make the chip card supply its identification word. The word comes out in two chunks: the first has 16 bits reserved for the answer-to-reset function, the second, 112 bits containing various data as described below

address	number	function
000	16	Answ...
016	8	111111... ...ry bits
024	4	manufacturer and first position of serial number 0000 ORGA 0 N1 1000 GDM 1 0100 ODS 2 1100 Gemplus 3 0010 Solaic 4 ... ... 1111 Reserve 16
028	4	checksum
032	4	value of the new card 1100 1,50 DM 0010 6,00 DM 1010 12,00 DM 1110 60,00 DM
036	4	year of manufacture and second position of serial number 0000 1980+10 N2 1000 1980+10 +1 0100 1980+10 +2 1100 1980+10 +3 0010 1980+10 +4 1010 1980+0(!) +5 ... ... 1111 1980+0 +16
040	4	month of manufacture (0...11) 0000 January +01 N3 N4 1000 February +02 0100 March +03 ... 1101 December +12 ... 1111 +16
048	4	serial number N9
052	4	serial number N8
056	4	serial number N7
060	4	serial number N6
064	8	residual value of card MSB number of 1-B a
072	8	residual value of card Bits b
080	8	residual value of card c
088	8	residual value of card d
096	8	residual value of card e residual value of card in pence $= a \cdot 8^4 + b \cdot 8^3 + c \cdot 8^2 + d \cdot 8^1 + e \cdot 8^0$
104	24	dummy bits 11111...1

950036 - 20

Table 3. Functions of the bits sent out by a disposable phonecard (having a fixed equivalent value). Example based on a Bundespost (German PTT) phonecard.

and shown in **Table 3**. The description is based on the assumption that a Bundespost (German PTT) telephone card is inserted into the reader.

Manufacturer (bits 24 through 27): a distinction is made between the manufacturers of the raw materials and the parts (chips) on the one hand, and the manufacturer of the assembly (the chip card itself) on the other.

Value of the new card: two different fields allow the card reader to establish the total value of the card at manufacture, and the remaining value (once credit units have been used up). The 'full' value of the card allows two different tariff rates to be used automatically, for instance, 25 pence per unit on a card worth £5, or 20 pence per unit on a card worth £20.

Date of manufacture: this indicates year and month of production. This is not the same as the date printed on the card.

Serial number: this is the serial number of the chip. It consists of nine numbers, N1 through N9. These numbers are appended to the previously mentioned information, and are read from bits 24 through 60.

Data encryption

Obviously, data on credit cards and, say, health insurance cards is strictly confidential and has to be protected against copying and other forms of misuse. Data on chip cards is therefore encrypted to one of the following standards:

- DES (data encryption standard), developed by IBM in 1977, is still among the simplest, safest and widest used algorithms.
- FES (fast data encryption standard) is a smaller version of DES using a shorter key. The system offers higher processing speed at the cost of reduced data security.
- DSA (digital signal algorithm), developed in 1991 by the NSA (National Security Agency) for the purpose of authenticity checking.
- IDEA (international data encryption algorithm), patent applied for in 1991.
- RSA Rivest, also known as the 'Shamir and Adleman public key' method.

When picking what looks like the best algorithm, the computing power of the microcontroller used should be taken into account to ensure a reasonable trade-off between the duration of read/write operations and data security.

Applications

Phonecards are available in two versions: cards with a credit function (where the cost of the call is automatically drawn from your bank or girobank account), and the far more successful cards with a fixed equivalent value or a fixed number of cost units, for instance, 10 or 50 units. Although not personalized, the latter are still unique because each one has a unique serial number. Instead of throwing used-up telephone cards away, it would be possible to use them as personal identification cards in a simple controlled access system to an office or an apartment building, with door locks controlled by a card reader and a microcontroller. Taking this a bit further, it would also be possible to extend such a system with a 'person in/out' recorder coupled with time logging.

(950036)

For further reading:

Amphenol, chip card product information C702-X, C703, C704, C705, C707, C708.
OKI, Smart Card product information.
ISO 177, DIN 66003, ISO 7810, ISO7811/1, ISO 7811/2, ISO 7811/3, ISO 7811/4, ISO 7811/5, ISO 7816-1, ISO7816-2, ISO7816-3, ISO 7816.
ANSI Data Encryption Algorithm 1, DES X3.92-1991.

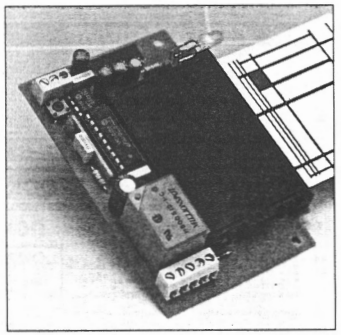


Fig. 7. An inexpensive and simple card reader with PCB contacts and an end switch.

JP1	JP2	JP2	Unit (h/min)	Total time
X	X	X	4 hours	40 hours
X	X	-	2 hours	20 hours
X	-	X	1 hour	10 hours
X	-	-	30 minutes	5 hours
-	X	X	15 minutes	2 hours 30 min.
-	X	-	10 minutes	1 hour 40 min.
-	-	X	5 minutes	50 minutes
-	-	-	1 minute	10 minutes

is not difficult, it does require accuracy and a little patience. Pay attention to proper isolation between the parts and the metal screening of the plug (which is connected to +5 V).

As with all mains-powered circuits, precautions should be taken to ensure electrical safety. In particular, the circuit must be earthed, so that it remains safe if the transformer or the relay breaks down. This precaution should always be observed, unless you are dealing with a double-isolated device, which is difficult to produce by a hobbyist. Here, the earthing is achieved by connecting the +5 V line to the earth pin of the mains plug. Although the mains voltage is only present at some points at the rear side of the PCB, you must always pull the mains plug before doing any work on the circuit.

Practical use

Fit jumpers JP1, JP2 and JP3 before you switch on the circuit. These jumpers set the length of a time unit. The total number of time units which can be charged is ten. The available options are shown in a separate box.

Jumper JP4, if fitted, gives a 'magnifying' effect during the last time unit. When the available time has dropped to one tenth of the total time, the LED scale is 'magnified' by ten, and the display starts to flash. This function is disabled when JP4 is not fitted. Your choice!

The circuit is adjustment-free. After taking it into use for the first time, you should start by making the 'master key'. This done by inserting a blank key, and then pressing the 'hidden' push-button, SW3. A user key is made as follows: insert a blank key, press SW3, and then SW1 ('down'). This produces a fully charged user key. If you leave this key inserted in the reader, the system starts to count down the time units until the load is switched off.

To charge a user key, first insert the master key (D3 lights), remove it, an then the user key. Next, adjust the number of time units to be given by means of push-buttons SW1 and SW2. Other keys are charged in the same way. The reader switches to normal mode automatically if there is no push-button activity within 10 seconds.

Although the construction and use of the Telly-Guard should be within reach of most of you, getting children to accept the principle of limited TV viewing time may present some fierce problems initially. (960304)

Note: the software mentioned in this article is available on floppy disk, see page 70.

```
S1110100A680B704A6FFB705A6...06A600AB
S111010EB712B713B714B716B71...18B71947
S111011CB71AB71BB71CB71DB723A614B71527
S111012AA650B720A614B722A6FFB721A662DE
S1110138B7081F091D099ACC0142CC01459A53
S11101469BA601B7233D1A270AA600B71ACDBF
S1110154028lCC0145B621A1C7220AB621279B
S1110162O6CD0287CC0178B621A1EE2606CD8B
S1110170O2B5CC01E3CC01459A9BA602B7234D
S111017E3D1A270DA600B71ACD02AECD0281A0
S1110180CCC0145B621A100270AA1EE2706A149
S1110190FF27022006CD02A5CC01B3CD047CC4
S11101A82606CD0291CC0178CC01789A9BA654
S11001B604B723B621A1EE2606CD02B5CC78
S11001C301E3B621A1C7220AB6212706CD0B
S10E01D00287CC0178CD047C2606CD0C
S11101DB02AECC0145CC01B39A9BA603B72318
S11101E93D19270DA600B719CD02BECD02CDDB
S11001F7CC0239B621A1EE2706CD02C4CCFE
S1110204020 9CC01E39A9BA605B723CD047C26
S1110212260 6CD02D6CC0145B621A1EE260665
S1110220CD02B5CC01E3B621A1EE270AA1FF61
S1110222706CD02CDCC0239CC02099A9BA63C
S1110230 6B723B621A1EE2706A1FF27022054
S110024A06CD02C4CC0209CD047C2606CDED
S1110257O2D6CC01453D19270DA600B719CDDE
S1110265O2EFCD02CDCC02393D18270DA600C4
S10F0273B718CD02DFCD02CDCC0239CC8F
S1110277F0239A6EECD0351811E00A601B7136D
S1110280CD048381CD0483B621270C4AA1C77A
S1110291B2302A6C7B721CD035181A60AB71FBF
S11102A9A600B71E811F00A600B713811E0019
S11102B7A601B713B71481A6C7CD035181A6C3
S11102C50AB71FA600B71E81A605B71FA60024
S11102D3B71E811F00A600B713B71481B62111
S11102E1AB14A1C72302A6C7B721CD035181D8
S11102EFB621A0142A06A1C72302A600B72137
S11002FDCD035181100299CD032CA680CDB4
S1110300339CD0343B710CD0343B7111502D9
S1110318102B61143B1102608A1C72306A195
S1110326EE2702A6FF81240414022002150211
S1110334120213028lAE0849CD032C5A26F999
S1110342811AE0812020702004913025A26F582
S1110350B1710100299CD032CA630CD0339CD
S111035E150211029D9D9D100299CD032CA63F
S110036C40CD0339B610CD0339B61043CD92
S1110379033915021102 9D9D9D10020702FD1D
S1110387110281010006A600B71C2014B61C4A
S1110395A1FF270E3C1CB61CA1022506A6FFE4
S11103A3B719B71C030006A600B71B2014B63A
S11103B11BA1FF270E3C1BB61BA1022506A6AE
S11103BFFFB718B71B050006A600B71D2014D3
S11103CDB61DA1FF270E3C1DB61DA10225067C
S11103DBA6FFB71AB71D8133173A152606A6DA
S11103E914B7153316B612A114241F0C001CF1
S11103F73D162704A6002014B612BB12BB123A
S1110405BB12BB12BB12BB12BB12BB12BB124A
S1110413 3D172734A1652504A601205AA151E6
S1110421 504A6812052A13D2504A6C1204A2F
S111042FA1292504A6E12042A1152504A6F169
S111043D203AA1012504A6F92032A6FD202EA6
S111044BA1B52504A60E201AA1A12504A61E03
S1110459 012A18D2504A63E200AA1792504B7
S1110467A67E2002A6FE3D132702A4F73D1434
S1110475 702A4FBB701813D1E26023D1F8114
S1110483B600444444A407A100260AA6D0B73C
S111049 1FA602B71E205CA104260AA668B7A7
S11104 9F1FA601B71E204EA102260AA6B4B75E
S11104AD1FA600B71E2040A106260AA65AB7B5
S11104BB1FA600B71E2032A101260AA62DB7E7
S11104C91FA600B71E2024A105260AA61EB7F2
S11104D71FA600B71E2016A103260AA60FB703
S11104E51FA600B71E2008A603B71FA600B767
S11104F31E81A662B7081F09B610B724B61101
S1110501B725CD03E2CD038A3A202618A65072
S111050FB7203D1E26043D1F270CB61FA00179
S1110511DB71FB61EA200B71E3A222613A6145C
S1110522BB722CD0301C70021A1FF2602A600BE
S1110539C700120F0905A601CC054DB624B764
S1110547 10B625B711809BC70010A6F2B701AD
S1110555CD0568C60010434848AA01B701CD81
S1110563 568CC0551A650B711A6FF4A26FD27
S10805713A1126F78198
S10407840769
S10907F804F501000100FC
S10507FE0100F4
S9030000FC
```

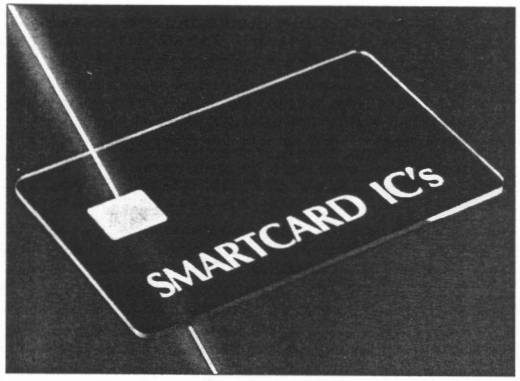
Fig. 4. Object code to be loaded into the microcontroller.

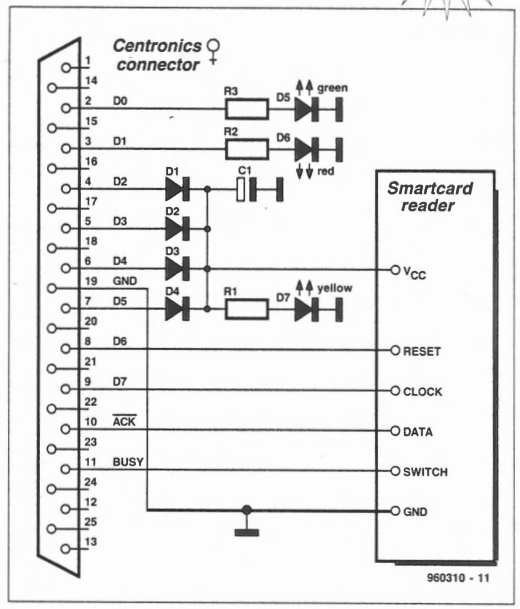
SMARTCARD READER

1st Prize (NL)

This design answers the widespread interest in applications involving smartcards. Chip-type telephone cards and credit cards catch the fancy of many. Those of you thinking of fraud at this point need not read any further, because that is not possible with this design. The circuit is, however, suitable for many other interesting applications, so don't throw away those expired telephone cards!

Design by P.H. Baars



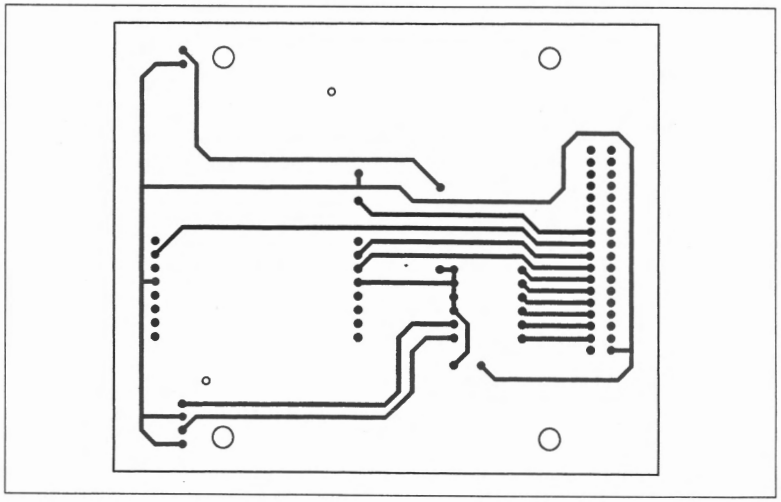


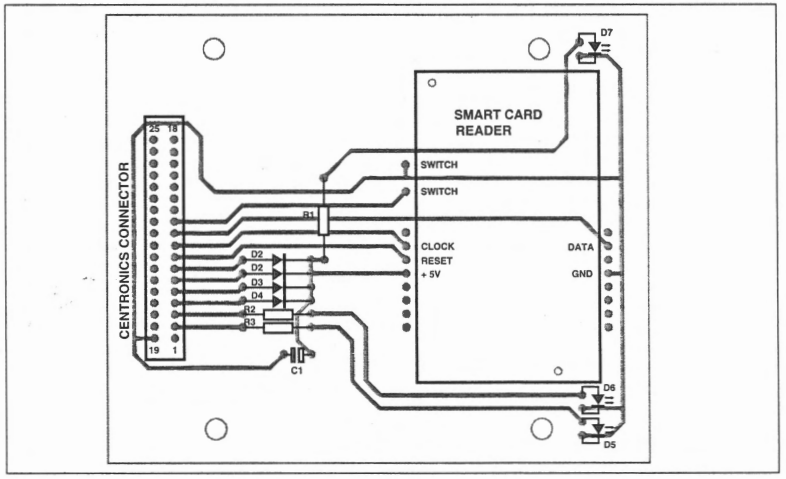
One application of the smartcard reader could be access protection to a program you have written yourself. This means that any user has to insert an authorized smartcard before he or she is allowed to use the program. Similarly, access checking and logging is within easy reach. Only a handful of parts are needed for experiments at home. The present design allows, for instance, telephone chip-cards to be read. The information read from such cards consists of the serial number, production date/month, and the remaining value.

The circuit diagram is so simple that a description is really superfluous. An external power supply is not needed because the supply voltage is stolen from the parallel port. Diodes D1 through D4 serve to prevent short-circuits between the databits. Databit 0 controls the green LED, databit 1 the red LED, and the yellow LED is connected to the power supply. The other databits are connected directly to the smartcard. The voltage is stabilized to some extent by electrolytic capacitor C1. The smartcard connections Clock and Reset are inputs, wile Data is an output.

The smartcard reader unit has a small internal switch which checks if a card is inserted. This switch is also connected to the Centronics port.

Having built the small board, you may check if it work with the aid of the test program (test.exe). If this test is passed, try 'cardtest.exe', which reads and decodes the ATR string.





COMPONENTS LIST

R1,R2,R3 = 1kΩ5
D1-D4 = 1N4148
C1 = 10µF 16V radial
LED1 = 3mm dia., yellow
LED2 = 3mm dia., red
LED3 = 3mm dia., green
Con1 = Centronics socket, PCB mount, angled pins.
Con2 = Smartcard reader unit. Available from eMedia GmbH, Postfach 610106, D-30601 Hannover, Germany. Price DM 12.

The program is relatively simple. There are various routines for the basic functions (LED on/off, clock high/low, etc.). The main program first checks if a card is inserted ('switch'). If so, data are read using the ATR (see Ref. 1), and checked. If this information is okay, it is converted into legible text.

The routine 'my_card' contains the registration number of one of my own telephone cards. The number may be replaced with your own number. The green LED will light when this number matches that on the card. If the numbers are different, the red LED lights.

The program is only intended as a starting point for further experiments, you can make it as intelligent and attractive as you like.

(960310)

Note: the software mentioned in this article is available on floppy disk, see page 70.

Reference:

1. Chip Cards, *Elektor Electronics* April 1995.

N-E-X-T M-O-N-T-H

another 16-page section of Elektor Electronics devoted to prize-winning entries from our International Circuit Design Competition 1995.
A selection from the subjects:

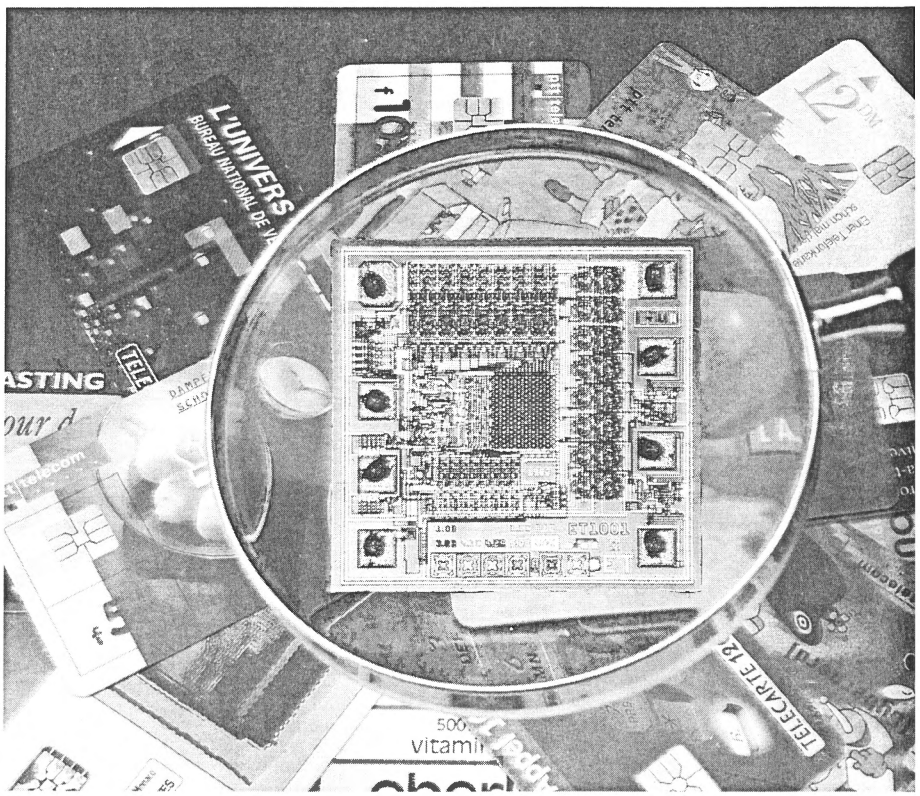
- **» Microcontroller Switching Clock RTC56**
- **» PC-Driven Battery Tester**
- **» 'Green power' for PCs**
- **» Hybrid Headphones Amplifier**
- **» Intelligent Motor Control for R/C Models**
- **» PWM Signal Generator**

Don't miss the February 1996 Issue!

focus on: chip cards

an exploratory look at intelligent telephone cards

Chip cards come in a wide variety, and their contents seems to exert a strong attraction on many electronics enthusiasts. Disposable telephone cards (some of which have become collector's items!) are a great starting point for many experiments in manipulating the electronics contained in the plastic. Some experimenters have successfully turned expired phonecards into electronic ID cards for use in controlled-access systems. Others, many on the 'hackers' front, use them to find weak spots in systems which have been declared totally secure.



By Patrick Gueulle

Whatever way you want to start examining the contents of an intelligent telephone card, you have to be able to communicate with the chip it contains. Communication, in turn, requires a basic knowledge of the signals transferred between the card and the reader unit. This knowledge, eventually, brings you to the actual thing: the contents of the memory on the card.

First: the hardware:

A chip card is a plastic card having the same size as a credit card. A very thin silicon chip is secured into the plastic carrier at an accurately determined position.

Awaiting the arrival and standardization of the contact-less chip card, the communication with the reader unit is accomplished via six, seven or eight flat contacts whose position is standardized.

The pin numbering of the chip contacts is shown in **Figure 1.** Actually, the proper term for the unit is 'micromodule'.

Although chips with eight contacts are still found occasionally, most modern cards have only six contacts, the ones designated ISO4 and ISO8 having disappeared.

Contact number ISO5 is always easy to locate. Representing the ground connection, it extends into the centre of the micromodule.

On the card, the chip may have two positions. The 'ISO' position shown in **Figure 2** is the most common these days, as it is the only one expected to survive in the long term.

The AFNOR variant shown in **Figure 3** is now obsolete, being a remnant of early telephone card series issued in France. Millions of these cards are still

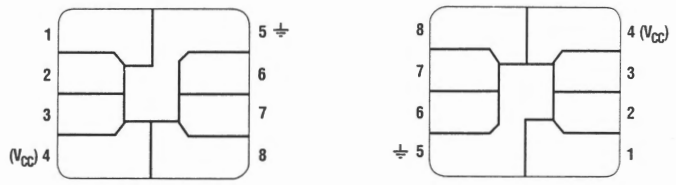


Figure 1. Terminal functions for ISO and AFNOR chip cards.

around, however. Not surprisingly, most commercially available card readers have two contact groups: one for ISO cards, and one for AFNOR cards. The contact groups are, incidentally, simply connected in parallel inside the cardreader.

Just like any other electronic component, a chip card has to be powered. The main supply voltage (V_{cc}) is +5 V. This is applied to contact ISO1.

The oldest cards around (manufactured in NMOS technology) require a second supply voltage, V_{pp}. Applied to contact ISO6, V_{pp} is normally at +5 V, or at +21 V during write operations.

With so few contacts left on the chip, it goes without saying that data is exchanged in serial fashion.

The ISO7 contact is reserved for data input/output (I/O). The use of the remaining contacts differs between card technologies.

Here, we limit ourselves to examine cards which are called 'synchronous', which covers disposable phone-cards. After all, these cards are really just protected memory units. By contrast, asynchronous cards contain a microprocessor. These cards are used for much more complex systems requiring a higher degree of security, such as pay-TV, credit cards and electronic wallets.

Synchronous chip cards operate in sequential fashion, using an internal address counter which always points at the bit which is to be read or written.

These 'micro-instructions' are written to the card via two or three contacts, one of which (in principle, ISO3), acts as a clock.

Virtually all telephone cards obey one of two communication protocols:

- the 'three-wire' protocol based on French technology (currently the most widely used in the world);
- the 'two-wire' protocol based on German technology (this is receiving gradual acceptance in Europe: including the UK, Holland, Switzerland, etc.,

Even a cursory look at the tables in **Figures 4 and 5** reveals the vast differences between these two protocols, which is another way of saying that they are incompatible.

None the less, the general procedure to launch a read operation on a card is largely identical for both protocols: first, the card is powered, and then, a 'RESET' micro-instruction is issued by the reader. Next, the first memory bit may be read via card contact ISO7.

Note, however, that there are cards (notably of the 2-wire type) which require a pull-up resistor to be present between the ISO7 contact and V_{cc}, because their output is of the 'open drain' type. In general, a resistor value between 5-kΩ and 10kΩ is sufficient.

In order to access the *n*th bit of the memory, the reader has to issue *n* 'UP' micro-instructions before it is able to read the relevant bit via the ISO7 contact.

Since no provision is made to decrement the address counter, access to any 'earlier' memory cell calls for a RESET and the relevant number of UP instructions to arrive at the desired address. So, bits are read in their original order for most of the time.

Under certain conditions deter-

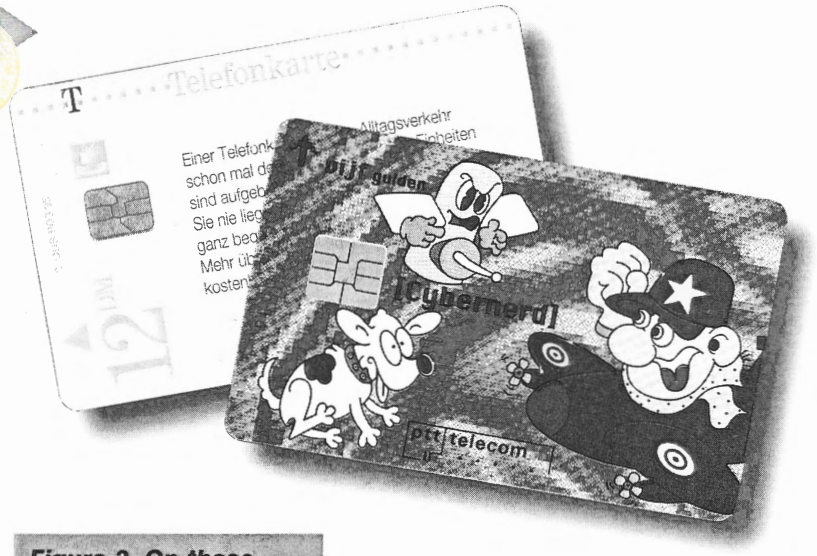
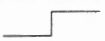


Figure 2. On these phone cards, the chip is in the ISO position.

Figure 3. Two AFNOR compatible phonecards.

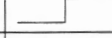
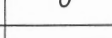
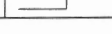
4 ***Figure 4. The 'French' protocol.***

ISO 6: Vpp (21V)
ISO 7: data output
ISO 8: fuse (do not use)

ISO 2:	ISO 4:	ISO 3:	micro-instruction
0	0		RESET
0	1		UP
1	1		PROGRAM (0→1)

5 ***Figure 5. The 'German' protocol.***

ISO 6: not connected
ISO 7: data

ISO 2:	ISO 3:	micro-instruction
1		RESET
0		UP
	0	PROGRAM (1→0) link these two sequences
0		

mined by the security logic implemented on the card, one specific instruction, PROGRAM, allows a card to be written to: that is, a 0 changed into a 1 on 'French' cards, or a 1 into a 0, on 'German' cards.

AND THEN: SOFTWARE

If different communication protocols are used for cards of the French and German type, then what about their memory contents?

A first-generation French phone card ("TeleCarte" in French) contains nothing but a 256-bit EPROM. Although all of these bits may be read, only the first 96 may be programmed by the factory because they are protected by an on-chip fuse (at the ISO8 contact) which is blown at the end of the production process.

This group of 96 bits is unique for each individual card: it contains a 'serial number' and an 'authentication message'. These two pieces of information allow each individual card to be recognized. Although the first and foremost aim of this protection is, of course, to prevent card cloning, the system also allows faulty cards to be detected.

This unique matrix is, of course, a godsend for anyone wanting to build, say, an electronic lock which only recognizes a few authorized cards. All you have to do is make the reader perform a check on the 96 bits. Bit numbers 8 through 15 in this block provide the 'application code' of the card. This code may have the hexadecimal value 03, 04, 05 or 06 for a French Telecard, while any value greater than or equal to 80 indicates a different application. The story behind this is that France Telecom has succeeded in forcing chip card manufacturers to pre-program bit 8 on cards intended for all other customers.

The entire area from location 96 through 255 is used for automatic counting of phone billing units. Initially, all bits are at 0, and these are replaced with 1's at a rate of billing units 'consumed' as you phone away.

In theory, the capacity of such a card would be 160 units. In practice, however, 10 units are 'burned' by the card factory for testing purposes, limiting the credit value of cards based on this technology to 150 phone billing units. In France, these cards have a value of 5, 50 or 120 units, which means that each expired (empty) Telecard still contains a number of bits which may be changed from 0 to 1 in the course of experimental manipulations.

Figure 7, for example, shows the memory contents of a new, unused 50-units phone card. The contents of the same card, but then empty, is given in **Figure 8** (note the 8 last bits which remain at logic 1 although all the card's worth has been used up). **Figure 9** shows how an appropriate piece of software is capable of deciphering the 256 bits on the card, and turn them

6

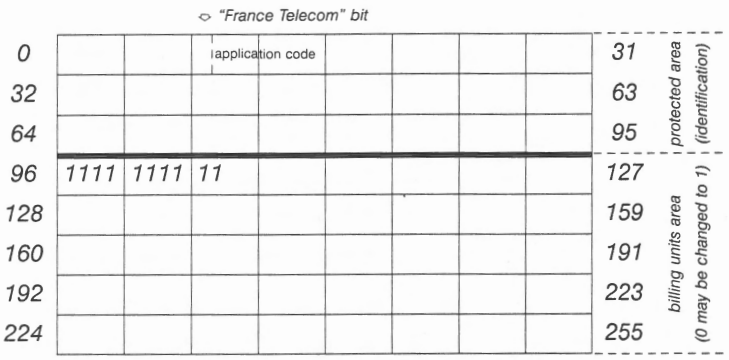


Figure 6. Memory structure of a French Telecard.

7 *Figure 7. French Telecard, 50 units, unused.*

1100	0011	0000	0101	0101	1001	0001	0100
1100	0011	0010	0010	1000	1000	0011	0011
1011	1111	1110	1110	0001	0000	0000	0110
1111	1111	1100	0000	0000	0000	0000	0000
0000	0000	0000	0000	0000	0000	0000	0000
0000	0000	0000	0000	0000	0000	0000	0000
0000	0000	0000	0000	0000	0000	0000	0000
0000	0000	0000	0000	0000	0000	0000	0000

8 *Figure 8. The same Telecard, empty.*

1100	0011	0000	0101	0101	1001	0001	0100
1100	0011	0010	0010	1000	1000	0011	0011
1011	1111	1110	1110	0001	0000	0000	0110
1111	1111	1111	1111	1111	1111	1111	1111
1111	1111	1111	1111	1111	1111	1111	0000
0000	0000	0000	0000	0000	0000	0000	0000
0000	0000	0000	0000	0000	0000	0000	0000
0000	0000	0000	0000	0000	0000	1111	1111

9

Chip Type:	Texas or EEPROM
Family Code:	05 (Phonecard)
Serial Number:	59142288
Authenticity Message:	33EE
Programming Parameters:	1 (50ms/21V)
Service Code:	0 (disposable card)
Total Value:	06 (50 units)
Used Up:	50 units
No Remaining Credit	

Figure 9. Interpretation (by a special program) of the data read from the card in Figure 8.

10

Figure 10. Memory counter of an empty Spanish Telecard, with an original worth 1,000 ptas.

1010	1011	1000	0011	1111	1111	1111	1111
0101	1010	0000	1001	1011	0111	0001	0101
0001	0100	1000	1010	0001	1110	0010	0010
1111	1111	1110	0010	0000	1000	0100	0001
0000	0100	0001	0000	0100	0001	0000	1000
0100	0000	1000	0100	0010	0000	1000	0001
0000	1000	0010	0110	1010	0001	1001	0010
1000	1010	0100	1001	0010	0100	1010	0001

11

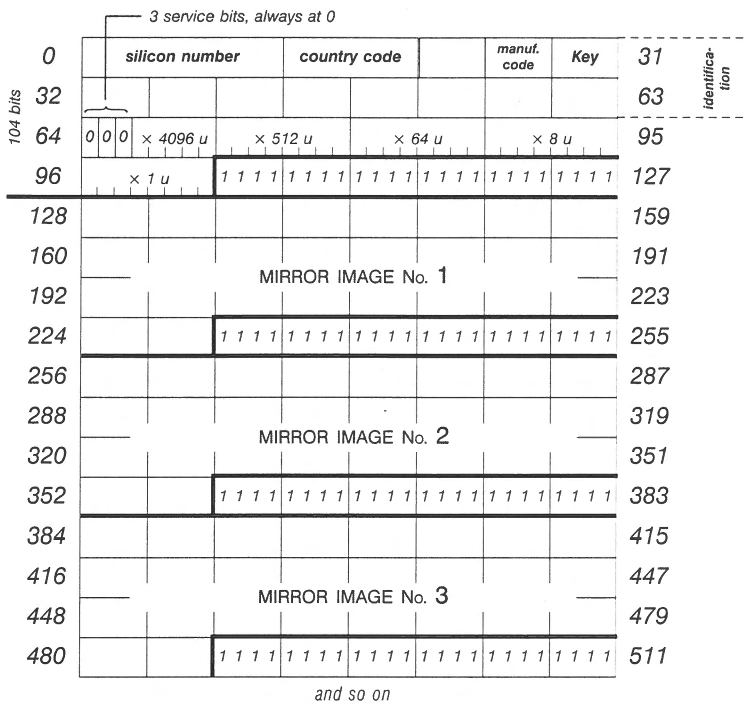


Figure 11. Memory structure of a German phonecard (old version).

Figure 12. Read result of the 512 bits in an empty German phonecard (old version). The same area of 128 bits appears four times.

1111	0010	0010	1111	1111	1111	0100	1010
1110	0010	1100	0000	1100	1110	0100	1100
0000	0000	0000	0000	0000	0000	0000	0000
0000	0000	1111	1111	1111	1111	1111	1111
1111	0010	0010	1111	1111	1111	0100	1010
1110	0010	1100	0000	1100	1110	0100	1100
0000	0000	0000	0000	0000	0000	0000	0000
0000	0000	1111	1111	1111	1111	1111	1111
1111	0010	0010	1111	1111	1111	0100	1010
1110	0010	1100	0000	1100	1110	0100	1100
0000	0000	0000	0000	0000	0000	0000	0000
0000	0000	1111	1111	1111	1111	1111	1111
1111	0010	0010	1111	1111	1111	0100	1010
1110	0010	1100	0000	1100	1110	0100	1100
0000	0000	0000	0000	0000	0000	0000	0000
0000	0000	1111	1111	1111	1111	1111	1111

into a maximum amount of meaningful data. Some countries (in particular, Spain and the Croatian Republic) use a much more intricate 'counting scheme' which allows the apparent limit of 150 units to be exceeded. Without going into details, this result may be explained by the fact that certain bits represent a value of several billing units, as illustrated by the example in **Figure 10** (memory contents of an empty Spanish phone card with an original value of 1,000 ptas).

Developed a couple of years after the French version, the German phone card ("Telefonkarte") has been able to benefit from a more modern technology, namely CMOS EEPROM.

However if you say EEPROM you also say 'possibility to erase and rewrite'. Also, the basic operation of these cards is radically different from the early French ones.

The table shown in **Figure 11** shows that the basic German phone card is set up around a memory of 104 bits. If you attempt to read bits 104 through 127, you invariably get 24 logic ones. From address 128 onwards, a mirror-image is found of the contents starting at 0. In other words, the address counter returns to the start in cyclic fashion. The first 64 bits may be compared to the first 96 on the French phonecard, in the sense that they also contain card identification data.

Bits 0 to 11 contain a 'silicon number' which is programmed in the chip when it is manufactured. This number may be the same in a (very) large number of cards.

The next eight bits are, in principle, identical for all cards from a nationwide operating telephone company (FF_h in Germany, $7F_h$ in Holland, BF_h in Guernsey, $2F_h$ in Great Britain, etc.).

Bits 24 to 27 identify the card maker, for example, 0_h for ORGA, 8_h for Giesecke & Devriendt, 4_h for ODS, C_h for Gemplus, 2_h for Soliac, 9_h for GPT, etc. For really unique data, however, we have to look in the area reserved for the billing units counter. This area is effectively divided into five counters: four of eight bits, and one of

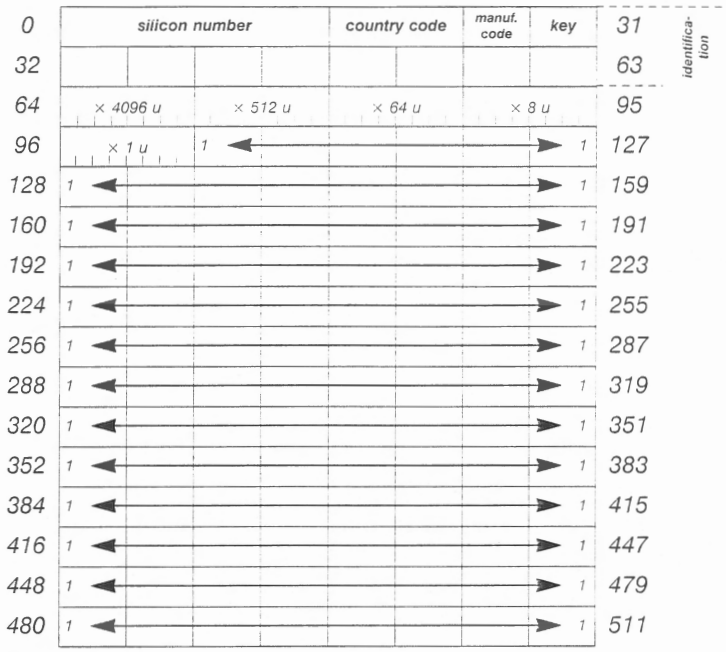


Figure 13. Eurochip memory structure.

five bits, whose function may be likened to that of an abacus. Each billing unit (or credit) you use up in a public phone booth is accounted for by a logic 1 changing into a 0 in the 'units' counter occupying the address range from 96 to 103. Once this area is full (in other words, when its eight bits are at logic 0), a bit is set to 0 in the next counter (the ×8 units one). This operation also resets the eight bits in the 'units' counter to logic 1. In the same way, a 'carry-over' is written into the ×64 units counter once the 8 units counter is emptied, and the same again with the last counter, which counts by 4,096 units.

Manufacturers of integrated circuits for use on chip cards always state that this 'counting scheme' allows a phone card to be produced representing a total of 20,480 phone billing units with just 37 bits (8×8×8×8×5 = 20,480).

A little arithmetic reasoning however reveals that the above is a gross error which no-one seems to have noticed for years! In actual fact, the capacity of the counter array is 25,160 units. Whatever the exact number, that's far more than the 160 units of a 256-bit EPROM card, and it real currency units like pence, cents or pfennigs to be counted directly, and not just those strange 0.80 FF units as in France. This advantage allows phone companies to charge calls depending on the actual duration (even down to seconds if so desired). On the down side, this technology has an Achilles heel in that it is possible for a user to re-charge his card himself, and so telephone for free. To prevent this kind of fraud, the card providers pre-load the counters in the factory, so that the 'units' which may be used up again are an exact match of the value printed on the card. So, on an 'empty' German phonecard (**Figure 12**), all bits of all counters are at 0.

This simple security measure was, apparently, not sufficient, witness the proposals for a more sophisticated technology designated 'Eurochip'.

Figure 13 shows that the first 128 bits are compatible with those we just examined. Only instead of three 'mirrored' areas, the memory area covering bit 128 to 511 contains only ones, interspersed with the occasional 0 as illustrated in **Figure 14**.

As you might well imagine, this area has a definite function in an encrypted security mechanism as, for instance, used in safes.

Top-secret for obvious reasons, this mechanism is based on the 'challenge-response' principle. The intention is to fit every public telephone booth with a security module in the form of a card containing a miniature chip. This module frequently sends a random number to the Telecard. This number is used by the card to perform a secret calculation.

Once returned to the security module, the result of the calculation is supposed to enable the module to run an error-free check on the authenticity of the card, and the financial transaction in progress.

There are now grave doubts whether the French T2G second-generation Telecard will ever make it to commercial use. This card employs a related mechanism, although it remains compatible with the 'first-generation' cards which are currently used in France.

At this point many Frenchmen will wonder if the arrival of a single European phone card, that is, one which is usable across all European borders (in as far as these exist), will mean the end of many years of pioneering research in their country. (960114)

Figure 14. Read result of the 512 bits in a Eurochip-based phonecard. The first 128 bits are compatible with the older versions.

1101	1000	0010	1111	1111	1100	0100	1010
1010	1010	0011	0100	1100	0001	1010	0110
0000	0000	0000	0000	0000	0000	0000	0000
0000	0000	1111	1111	1111	1111	1111	1111
1111	1111	1111	1111	1111	1111	1111	1111
1111	1111	1111	1111	1111	1111	1111	1111
1111	1111	1111	1111	1111	1111	1111	1111
1111	1111	1111	1111	1111	1111	1111	1111
1111	1111	1111	1111	1111	1111	1111	1111
1111	1111	1111	1111	1111	1111	1111	1111
0111	1111	1111	1111	1111	1111	1111	1111
1111	1111	1111	1111	1111	1111	1111	1111
1111	1111	1111	1111	1111	1111	1111	1111
1111	1111	1111	1111	1111	1111	1111	1111
1111	1111	1111	1111	1111	1111	1111	1111
1111	1111	1111	1111	1111	1111	1111	1111